Abstract

Methods and apparatus for enhanced CMEA, or ECMEA, processing. A forward ECMEA and a reverse ECMEA process are provided. The forward ECMEA process decrypts text encrypted by the reverse ECMEA process and the reverse ECMEA process decrypts text encrypted by the forward ECMEA process. The forward ECMEA process employs a first transformation, an iteration of the CMEA process, and a second transformation. The reverse ECMEA process employs a first inverse transformation, an iteration of the CMEA process, and a second inverse transformation. The transformations and inverse transformations, and the iterations of the CMEA process, employ secret offsets to improve security. The transformations and the iteration of the CMEA process also employ an enhanced tbox function using an involutary lookup table.